

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328117

(43)Date of publication of application : 30.11.1999

(51)Int.Cl. G06F 15/00
G06F 13/00
G09C 1/00
G09C 1/00
H04L 9/32

(21)Application number : 10-131491

(71)Applicant : HITACHI LTD

(22)Date of filing : 14.05.1998

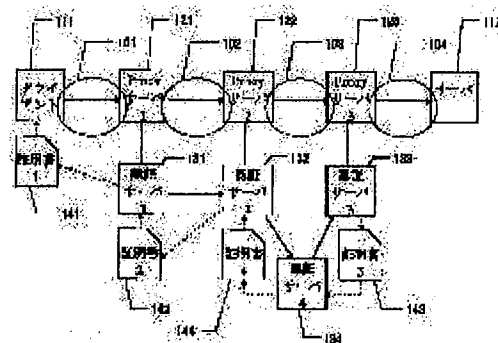
(72)Inventor : MURAKAMI HIROMASA

(54) USER MANAGING METHOD OF AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the system which eliminates the need to register user information on a client to an authentication server that all proxy servers repeating signals between the client and a server belong to.

SOLUTION: Only the authentication server 131 which is closest to a client 111 registers the user and for subsequent authentication, certificates are handed over between authentication servers. When the client 111 connects to a server 112, authentication is done between the client 111 and the authentication server which is closest to it and then authentication is performed between authentication servers to hand over the certificate of the client 111; when the certificate reaches the authentication server that the proxy server 123 closest to the server 112 belongs to, route information is sent to the client. The client 111 performs authentication with the proxy server according to the route information to establish a connection up to the server 112 to the end.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application]

converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-328117

(43)公開日 平成11年(1999)11月30日

(51)Int.Cl.⁶ 識別記号

G 0 6 F 15/00 3 3 0

13/00 3 5 1

G 0 9 C 1/00 6 4 0

6 6 0

H 0 4 L 9/32

F I

G 0 6 F 15/00 3 3 0 A

13/00 3 5 1 Z

G 0 9 C 1/00 6 4 0 Z

6 6 0 E

H 0 4 L 9/00 6 7 5 A

審査請求 未請求 請求項の数3 O L (全 10 頁)

(21)出願番号 特願平10-131491

(22)出願日 平成10年(1998) 5月14日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 村上 弘真

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

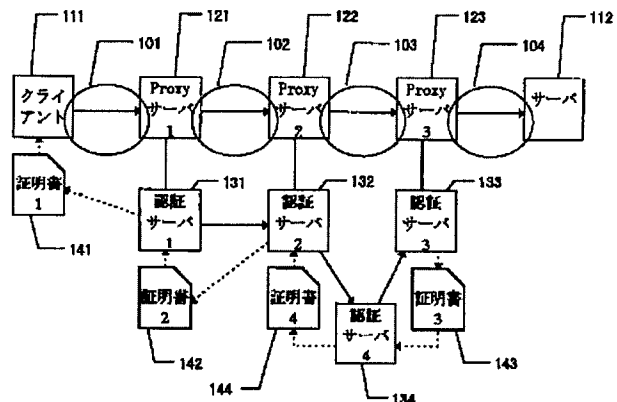
(74)代理人 弁理士 矢島 保夫

(54)【発明の名称】 認証システムにおけるユーザ管理方法

(57)【要約】 (修正有)

【課題】クライアントとサーバの間を中継する全てのプロキシサーバの属する認証サーバへクライアントのユーザ情報を登録する必要がある方式を提供する。

【解決手段】ユーザ登録をクライアントに最も近い認証サーバのみにし、それ以降の認証には認証サーバ間で証明書を受け渡すようにする。クライアントからサーバに接続する際には、クライアントとそれに最も近い認証サーバとの間で認証を行なった後、認証サーバ間で認証を行なってクライアントの証明書を受け渡していき、サーバに最も近いプロキシサーバが属する認証サーバまで辿り着いたら、経路情報をクライアントに送る。クライアントは、経路情報にしたがってプロキシサーバとの間で認証を行ない、最終的にサーバまでの接続を確立する。



【特許請求の範囲】

【請求項1】 ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、

あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくとともに、

あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくことを特徴とする認証システムにおけるユーザ管理方法。

【請求項2】 ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、

あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくステップと、

あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくステップと、

前記クライアントから前記サーバに接続するとき、前記クライアントから該クライアントに最も近い認証サーバに接続して認証を行なうステップと、

前記クライアントに最も近い認証サーバから、次に中継するプロキシサーバの属する認証サーバへ、接続し、認証サーバ間で受け渡した証明書を用いて認証サーバ間の認証を行なうとともに、前記クライアントの証明書を受け渡し、これを要求受付先のサーバに最も近いプロキシサーバの属する認証サーバに辿り着くまで繰り返すことにより、前記クライアントからサーバへ接続する際に中継するプロキシサーバの経路情報を取得するステップと、

中継するプロキシサーバの経路情報を前記クライアントに送るステップと、

前記経路情報に基づいて、前記クライアントと前記プロキシサーバとの間の認証を行なっていくことにより、前記クライアントと前記サーバ間の接続を確立するステップとを備えたことを特徴とする認証システムにおけるユーザ管理方法。

【請求項3】 前記中継するプロキシサーバを、階層化した認証サーバで管理することを特徴とする請求項1または2の何れか1つに記載の認証システムにおけるユーザ管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、仮想プライベートネットワーク（Virtual Private NetWork:VPN）に必要な認証を秘密鍵暗号方式を用いて実行するために用いるユーザ情報の管理作業、およびVPNにおいてクライアントからサーバへ到達するために中継するプロキシ（Proxy）サーバの設定管理作業を軽減する、管理方法に関する。

【0002】

【従来の技術】 近年、インターネットから社内イントラネットへアクセスする等、公衆回線を使って安価にネットワークシステムを構築するニーズが高まっている。インターネットを介して、あたかも一つの企業内ネットワークに見せるシームレスな接続を提供するのがVPNである。VPNでは、なりすましを防ぐためにユーザ認証を行ってからデータの送受信を開始し、また盗聴や改竄から公衆回線を流れるデータを守るために暗号化する機能を持つ。

【0003】 VPNの構成要素は、要求元のクライアント、要求受付先のサーバ、該クライアントおよびサーバ間の公衆回線を流れるデータを暗号化／復号するプロキシサーバ、および、認証要求を受けてユーザの認証とユーザ管理を行う認証サーバに大別される。

【0004】 従来の秘密鍵暗号方式による認証では、例えば特開平09-069831号「暗号通信システム」に示されるように、クライアントからプロキシサーバに接続すると、プロキシサーバの属する認証サーバが持つユーザ情報と、認証サーバからクライアントに配布した証明書とを元にして、認証が行われる。そのため、クライアントとサーバとの間で複数のプロキシサーバを中継する場合、全てのプロキシサーバの属する認証サーバから事前にクライアントへ証明書が配布されていなければいけない。

【0005】 また、要求元のクライアントから目的の要求受付先のサーバに接続するために、どのプロキシサーバを中継しなければいけないかを、事前に全てのプロキシサーバへ定義しておかなければいけなかった。

【0006】

【発明が解決しようとする課題】 上記従来技術では、要求元のクライアントと要求受付先のサーバの間を中継する全てのプロキシサーバの属する認証サーバへ、当該クライアントのユーザを登録しなければいけないことになる。多数のユーザが利用する、複数のプロキシサーバが存在するネットワーク環境では、ユーザの管理だけで多大な作業が必要になり、それぞれの認証サーバから発行された証明書を、発行先のユーザへ配布しなければいけない問題があった。また、要求元のクライアントから要求受付先のサーバまでの経路を事前に全てのプロキシサーバへ定義しておかなければならぬ面倒であった。

【0007】 本発明は、上述の従来技術における問題点を鑑み、クライアントとサーバの間を中継する全てのプ

ロキシサーバの属する認証サーバへ当該クライアントのユーザのユーザ情報を登録する必要がなく、また経路を事前に全てのプロキシサーバへ定義しておく必要もないような認証システムにおけるユーザ管理方法を提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するため、請求項1に係る発明は、ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくとともに、あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくことを特徴とする。

【0009】請求項2に係る発明は、ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくステップと、あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくステップと、前記クライアントから前記サーバに接続するとき、前記クライアントから該クライアントに最も近い認証サーバに接続して認証を行なうステップと、前記クライアントに最も近い認証サーバから、次に中継するプロキシサーバの属する認証サーバへ、接続し、認証サーバ間で受け渡した証明書を用いて認証サーバ間の認証を行なうとともに、前記クライアントの証明書を受け渡し、これを要求受付先のサーバに最も近いプロキシサーバの属する認証サーバに辿り着くまで繰り返すことにより、前記クライアントからサーバへ接続する際に中継するプロキシサーバの経路情報を取得するステップと、中継するプロキシサーバの経路情報を前記クライアントに送るステップと、前記経路情報に基づいて、前記クライアントと前記プロキシサーバとの間の認証を行なっていくことにより、前記クライアントと前記サーバ間の接続を確立するステップとを備えたことを特徴とする。

【0010】請求項3に係る発明は、請求項1または2において、前記中継するプロキシサーバを、階層化した認証サーバで管理することを特徴とする。

【0011】

【発明の実施の形態】以下、図面を参照して本発明の実

施の形態を説明する。

【0012】本実施の形態では、証明書の発行（ユーザの登録）をクライアントに最も近い認証サーバのみにし、ユーザ情報の管理作業を軽減する。証明書を発行した認証サーバ以外の認証サーバとの認証は、クライアントに最も近い認証サーバから次に中継するプロキシサーバの属する認証サーバへ、クライアントの証明書を認証サーバ間で順次受け渡し、クライアントの認証に使用する。また、要求受付先のサーバに最も近いプロキシサーバの属する認証サーバにたどりついた時点で、中継するプロキシサーバの情報をクライアントへ送り、その情報を元にクライアントと各認証サーバ間の認証を行っていく。

【0013】上記の方式を実現するため、本実施の形態では、認証サーバ間で認証を行い、証明書を受け渡す機能を持つ。また中継するプロキシサーバの定義と次に中継するプロキシサーバが属する認証サーバの定義を認証サーバに持たせ、中継するプロキシサーバの検索は認証サーバが行う。さらに認証サーバは階層構造を持たせることにより、次に中継するプロキシサーバが属する認証サーバの定義の管理作業を軽減させる。

【0014】以下、本実施の形態を詳しく説明する。なお、本実施の形態は、クライアントからサーバへの接続に3台のプロキシサーバを中継し、それぞれのプロキシサーバが属する認証サーバが3台あり、認証サーバ2, 3が属する上位の認証サーバ4が存在するシステムを例として説明する。

【0015】図1は、本実施の形態のシステム構成図である。図1において、ネットワーク環境は、ネットワーク1, 2, 3, 4（101, 102, 103, 104）で独立したネットワークである。各プロキシサーバ（121, 122, 123）とそれの属する認証サーバ（131, 132, 133）は、同一ネットワーク内にある。

【0016】次に、要求元であるクライアント（111）について説明する。クライアント（111）は、サーバ（112）に接続してデータを送受信する形態のアプリケーションが動作するクライアントである。VPNの設定として、サーバ（112）に接続するにはプロキシサーバ1（121）を中継するという情報のみがクライアント（111）にあらかじめ定義されており、認証サーバ1（131）から証明書（141）が配布済みである。クライアント（111）上のアプリケーションからサーバ（112）への接続要求があると、クライアント（111）はプロキシサーバ1（121）に接続して、認証サーバ1（131）との認証を行う。図5に、クライアントのVPNとしての動作を示す。図5の手順については後に詳述する。

【0017】次に、要求受付先であるサーバ（112）について説明する。サーバ（112）ではアプリケーション

ョンサーバが起動して、クライアント（１１１）からの接続を待機している。

【００１８】次に、プロキシサーバ１～３（１２１～１２３）について説明する。クライアント（１１１）に最も近いのがプロキシサーバ１（１２１）であり、ネットワーク１（１０１）と２（１０２）とを中継し、クライアント（１１１）から最初に認証要求のあるプロキシサーバである。サーバ（１１２）に最も近いプロキシサーバがプロキシサーバ３（１２３）であり、ネットワーク３（１０３）と４（１０４）とを中継し、サーバ（１１２）と平文データの送受信を行う、中継の終端となるプロキシサーバである。プロキシサーバ２（１２２）は、ネットワーク２（１０２）と３（１０３）とを中継するプロキシサーバである。図６に、これらのプロキシサーバの動作を示す。図６の手順については後に詳述する。

【００１９】次に、認証サーバ１～４（１３１～１３４）について説明する。プロキシサーバ１（１２１）、２（１２２）、３（１２３）が属する認証サーバが、それぞれ認証サーバ１（１３１）、２（１３２）、３（１３３）となる。ここでは１台のプロキシサーバが１台の認証サーバに属する場合を例として説明するが、複数台のプロキシサーバが１台の認証サーバに属することも可能である。認証サーバ１（１３１）は独立した１台の認証サーバであるが、認証サーバ２（１３２）、３（１３３）は認証サーバ４（１３４）が統括する認証サーバグループを形成している。認証サーバ４は、この認証サーバグループ内の認証サーバ２（１３２）、３（１３３）を統括する。

【００２０】各認証サーバには、クライアント（１１１）からサーバ（１１２）に接続するために次に中継すべきプロキシサーバが属する認証サーバを定義した中継経路定義情報が登録されている。図２に、その中継経路定義情報を示す。図２に示すように、認証サーバ１（１３１）には、サーバ（１１２）への接続要求が来たとき、次に中継すべきプロキシサーバの情報を持っているのが認証サーバ２（１３２）であることを示す中継経路定義情報が登録されている。認証サーバ２（１３２）には、中継経路定義情報は登録されていない。認証サーバ３（１３３）には、サーバ（１１２）への接続要求が来たとき、次にサーバ（１１２）と直接データの送受信が可能であることを示すEndが登録されている。認証サーバ４（１３４）には、サーバ（１１２）への接続要求が来たとき、次に中継すべきプロキシサーバの情報を持っているのが認証サーバ３（１３３）であることを示す中継経路定義情報が登録されている。

【００２１】各認証サーバには、クライアント（１１１）からサーバ（１１２）に接続するために接続を中継するプロキシサーバ（各認証サーバが管理するプロキシサーバ）を示す定義情報が登録されている。図３に、その定義情報が示す。図３に示すように、認証サーバ１

（１３１）には、サーバ（１１２）への接続要求が来たとき、この認証サーバ１（１３１）で管理され、その接続要求を中継するプロキシサーバが、プロキシサーバ１（１２１）であることを示す定義情報が登録されている。認証サーバ２（１３２）には、サーバ（１１２）への接続要求が来たとき、この認証サーバ２（１３２）で管理され、その接続要求を中継するプロキシサーバが、プロキシサーバ２（１２２）であることを示す定義情報が登録されている。認証サーバ３（１３３）には、サーバ（１１２）への接続要求が来たとき、この認証サーバ３（１３３）で管理され、その接続要求を中継するプロキシサーバが、プロキシサーバ３（１２３）であることを示す定義情報が登録されている。認証サーバ４（１３４）には、そのような定義情報は登録されていない。

【００２２】各認証サーバには、認証サーバのグループを構成する上位の認証サーバを定義する定義情報が登録されている。図４に、その定義情報を示す。図４に示すように、認証サーバ２（１３２）には、自認証サーバの上位の認証サーバとして認証サーバ４（１３４）が登録されている。認証サーバ３（１３３）には、自認証サーバの上位の認証サーバとして認証サーバ４（１３４）が登録されている。認証サーバ１（１３１）および４（１３４）には、上位の認証サーバが登録されていない。

【００２３】クライアント（１１１）からサーバ（１１２）への接続は、認証サーバ１（１３１）が持つ証明書（認証サーバ１（１３１）がクライアント（１１１）に発行した証明書１（１４１））を中継経路定義に従って次の認証サーバへと順次送り、各認証サーバは一時的に証明書を保管し、クライアント（１１１）との認証に用いる。認証サーバ間の認証に使用する証明書は、事前に認証を要求する相手から配布されている必要がある。この例では、認証サーバ１（１３１）はあらかじめ認証サーバ２（１３２）が発行した証明書２（１４２）の配布を受けており、認証サーバ２（１３２）はあらかじめ認証サーバ４（１３４）が発行した証明書４（１４４）の配布を受けており、認証サーバ３（１３３）はあらかじめ認証サーバ４（１３４）が発行した証明書３（１４３）の配布を受けているものとする。接続を中継する次の認証サーバが、透過でない独立した別のネットワークに存在する場合、認証はプロキシサーバを中継して行われる。図７、図８、および図９に、認証サーバの動作を示す。図７、図８、および図９の手順については、後に詳述する。

【００２４】上記の環境で、クライアント（１１１）からサーバ（１１２）に対して接続要求があるときの処理手順を、図５～図９のフローチャートを参照して説明する。

【００２５】クライアント（１１１）からサーバ（１１２）に対して接続要求があると、クライアント（１１１）は図５の処理を開始する。まず、サーバ（１１

2)へ接続するのに中継するプロキシサーバを検索し(ステップ501)、当該プロキシサーバへ接続する(ステップ502)。クライアント(111)は、サーバ(112)に接続するためには、プロキシサーバ1(121)を中継すべきことを知っているので、VPNはプロキシサーバ1(121)へ接続し、認証を開始する(ステップ503)。すなわち、ステップ503で、プロキシサーバ1(121)へ、証明書1(141)を付けてクライアント(111)の認証要求を送信する。

【0026】プロキシサーバ1(121)は、図6の処理で接続待ち状態になっているので、クライアント(111)からの証明書1(141)付きの認証要求を受信し(ステップ601)、プロキシサーバ1(121)が属する認証サーバ1(131)へ接続し(ステップ602)、クライアント(111)の認証要求を証明書1(141)を付けて送信する(ステップ603)。

【0027】認証サーバ1(131)は、図7の処理で接続待ち状態になっているので、プロキシサーバ1(121)からのクライアント認証要求を受信し(ステップ701)、証明書1(141)と認証サーバ1(131)が管理するユーザ情報と比較して認証を行う(ステップ702)。認証に失敗したときは、コネクションを切断して(ステップ704)、接続待ちに戻る。認証に成功したときは、認証要求元を判定し(ステップ703)、認証要求元がクライアントからのときは、図8のステップ801に進み、認証要求元が認証サーバからのときは、図9のステップ901に進む。いまはクライアント(111)からの認証要求であるので、図8の処理を実行する。

【0028】まず、証明書の種別を判別する(ステップ801)。クライアント(111)から送られてきた証明書1(141)は、いま処理を行なっている認証サーバ自らが発行したものであるから、ステップ802に進む。そして、次の認証サーバの情報を中継経路定義情報(図2)から検索する(ステップ802)。図2から分かるように、認証サーバ1(131)には、接続先がサーバ(112)である接続要求が来たとき、次の認証サーバは認証サーバ2(132)である旨が登録されている。そこで、検索結果として認証サーバ2(132)を得て、ステップ803からステップ805に進み、認証サーバ1(131)から認証サーバ2(132)へ接続し、証明書2を付けて認証サーバ2(132)に認証要求を送信する(ステップ805)。

【0029】認証サーバ2(132)は、図7の処理で接続待ち状態になっているので、認証サーバ1(131)からの認証要求を受信し(ステップ701)、認証サーバ1(131)から送信された証明書2(142)と認証サーバ2(132)が管理する認証サーバ情報とを比較して認証を行う(ステップ702)。認証に失敗したときは、コネクションを切断して(ステップ704)、接続待ちに戻る。認証に成功したときは、認証要求元を判定する(ステップ703)。いまは認証要求元が認証サーバ2(132)からであるので、認証は成功し、図9の処理を実行することになる。

4)、接続待ちに戻る。認証に成功したときは、認証要求元を判定する(ステップ703)。いまは認証要求元が認証サーバ1(131)からであるので、認証は成功し、図9の処理を実行することになる。

【0030】認証サーバ2(132)における認証に成功したので、認証サーバ1(131)における処理は、ステップ805からステップ806を経て、ステップ808に進む。ここでクライアント(111)の証明書1(141)を、次の認証サーバである認証サーバ2(132)に送信し(ステップ808)、中継経路受信待ちに入る(ステップ809)。

【0031】認証サーバ2(132)における図9の処理では、まず、クライアントの証明書1(141)を認証サーバ1(131)から受信して一時的に保存し(ステップ901)、次の認証サーバを中継経路定義情報

(図2)から検索する(ステップ902)。検索した結果、認証サーバ2(132)には、サーバ(112)に対する次の認証サーバは登録されていないが、上位の認証サーバが定義(図4)されているため、ステップ903から904を経て、ステップ905に進み、認証サーバ4(134)へ接続し、証明書4を付けて認証サーバ4(134)に認証要求を送信する(ステップ905)。

【0032】認証サーバ4(134)は、図7の処理で接続待ち状態になっているので、認証サーバ2(132)からの認証要求を受信し(ステップ701)、認証サーバ2(132)から送信された証明書4(144)と認証サーバ4(134)が管理する認証サーバ情報とを比較して認証を行う(ステップ702)。認証に失敗したときは、コネクションを切断して(ステップ704)、接続待ちに戻る。認証に成功したときは、認証要求元を判定する(ステップ703)。いまは認証要求元が認証サーバ2(132)からであるので、認証は成功し、図9の処理を実行することになる。

【0033】認証サーバ4(134)における認証に成功したので、認証サーバ2(132)における処理は、ステップ905からステップ906を経て、ステップ908に進む。ここでクライアント(111)の証明書1(141)を、次の認証サーバである上位の認証サーバ4(134)に送信し(ステップ908)、中継経路受信待ちに入る(ステップ909)。

【0034】認証サーバ4(134)における図9の処理では、まず、クライアントの証明書1(141)を認証サーバ2(132)から受信して一時的に保存し(ステップ901)、次の認証サーバを中継経路定義情報(図2)から検索する(ステップ902)。検索した結果、認証サーバ4(134)には、次の認証サーバは認証サーバ3(133)である旨が登録されている。そこで、ステップ903から905に進み、次の認証サーバ2(132)へ接続し、証明書2を付けて認証サーバ2(132)に認証要求を送信する(ステップ905)。

(133)に認証要求を送信する(ステップ905)。

【0035】認証サーバ3(133)は、図7の処理で接続待ち状態になっているので、認証サーバ4(134)からの認証要求を受信し(ステップ701)、認証サーバ4(134)から送信された証明書3(143)と認証サーバ3(133)が管理する認証サーバ情報とを比較して認証を行う(ステップ702)。認証に失敗したときは、コネクションを切断して(ステップ704)、接続待ちに戻る。認証に成功したときは、認証要求元を判定する(ステップ703)。いまは認証要求元が認証サーバ4(134)からであるので、認証は成功し、図9の処理を実行することになる。

【0036】認証サーバ3(133)における認証に成功したので、認証サーバ4(134)における処理は、ステップ905からステップ906を経て、ステップ908に進む。ここでクライアント(111)の証明書1(141)を、次の認証サーバである認証サーバ3(133)に送信し(ステップ908)、中継経路受信待ちに入る(ステップ909)。また、認証サーバ4(134)では、クライアント(111)の認証を行なわないため、証明書1(141)を一時保存しておく必要が無いから、証明書1は破棄する。

【0037】認証サーバ3(133)における図9の処理では、まず、クライアントの証明書1(141)を認証サーバ4(134)から受信して一時的に保存し(ステップ901)、次の認証サーバを中継経路定義情報

(図2)から検索する(ステップ902)。検索した結果、次の認証サーバは無く、Endが検出されるから、中継するプロキシサーバ3(123)の情報(図3)を認証サーバ4(134)へ中継経路情報として送信し(ステップ910)、コネクションを切断する。

【0038】認証サーバ4(134)は、図9のステップ909で中継経路受信待ち状態にあるが、認証サーバ3(133)から送られてきた中継経路情報(サーバ(112)に接続するために最後に中継するプロキシサーバがプロキシサーバ3(123)であることを示す情報)を受信して(ステップ909)、該受信した中継経路情報を、認証要求元である認証サーバ2(132)へ送信し(ステップ910)、コネクションを切断する。なお、この認証サーバ4(134)におけるステップ910では、中継経路情報に何も付け加えない。図3から分かるように、認証サーバ4(134)には、中継するプロキシサーバの登録が無いからである。

【0039】認証サーバ2(132)は、図9のステップ909で中継経路受信待ち状態にあるが、認証サーバ4(134)から送られてきた中継経路情報を受信して(ステップ909)、該受信した中継経路情報に、中継するプロキシサーバ2(122)の情報(図3)を付加して、認証要求元である認証サーバ1(131)へ送信し(ステップ910)、コネクションを切断する。結局

として、認証サーバ1(131)に送られる中継経路情報は、「サーバ(112)に接続するためには、プロキシサーバ2, 3の順に中継する」という情報になる。

【0040】認証サーバ1(131)は、図8のステップ809で中継経路受信待ち状態にあるが、認証サーバ2(132)から送られてきた中継経路情報を受信して(ステップ809)、該受信した中継経路情報をプロキシサーバ1(121)へ送信し(ステップ810)、さらに認証成功を示す情報をプロキシサーバ1(121)へ送信する(ステップ811)。そして、ステップ704に進み、コネクションを切断する。

【0041】プロキシサーバ1(121)は、認証サーバ1(131)から認証成功の通知を受信すると、ステップ604から605に進み、クライアント(111)に、認証の成功と共に、中継するプロキシサーバがプロキシサーバ2, 3であることを通知する(ステップ605)。また、クライアント(111)から次の中継先であるプロキシサーバ2への接続要求を受信すると(ステップ607)、プロキシサーバ2へ接続して、データの中継を開始する(ステップ608)。

【0042】クライアント(111)は、プロキシサーバ1(121)からの認証成功の通知を受信すると、ステップ504から505に進み、次に中継するプロキシサーバがプロキシサーバ2(122)であるから、プロキシサーバ1(121)を中継して、プロキシサーバ2(122)へ接続要求を送信し(ステップ506)、証明書1(141)を付けてプロキシサーバ2(122)へクライアントの認証要求を送信する(ステップ503)。

【0043】プロキシサーバ1(121)は、ステップ608でデータを中継する状態にあるから、クライアント(111)からのプロキシサーバ2(122)への接続要求、および認証要求は、プロキシサーバ1(121)を経て、プロキシサーバ2(122)へ送られる。

【0044】プロキシサーバ2(122)は、図6の処理で接続待ち状態になっているので、クライアント(111)からの証明書1(141)付きの認証要求を受信し(ステップ601)、プロキシサーバ2(122)が属する認証サーバ2(132)へ接続し(ステップ602)、クライアント(111)の認証要求を証明書1(141)を付けて送信する(ステップ603)。

【0045】認証サーバ2(132)は、図7の処理で接続待ち状態になっているので、プロキシサーバ2(122)からのクライアント認証要求を受信し(ステップ701)、受信した証明書1(141)を用いて認証を行う(ステップ702)。認証サーバ2(132)では上述した処理により証明書1(141)が一時保存されているので認証は成功し、ステップ702から703に進む。また、認証要求元はクライアントであるので、図8の処理に進む(ステップ702)。図8において、証

明書種別の判定（ステップ801）では、受け取った証明書1（141）は認証サーバ2（132）が管理する証明書ではないため、中継経路定義の検索は行わず、認証が成功した時点でプロキシサーバ2（122）へ認証の成功を送信する（ステップ811）。認証終了後は、認証サーバ2（132）は証明書1（141）を破棄する。

【0046】プロキシサーバ2（122）は、認証サーバ2（132）から認証成功の通知を受信すると、ステップ604から605に進み、クライアント（111）に、認証の成功を通知する（ステップ605）。また、クライアント（111）から次の中継先であるプロキシサーバ3への接続要求を受信すると（ステップ607）、プロキシサーバ3へ接続して、データの中継を開始する（ステップ608）。

【0047】クライアント（111）は、プロキシサーバ2（122）からの認証成功の通知を受信すると、ステップ504から505に進み、次に中継するプロキシサーバがプロキシサーバ3（123）であるから、プロキシサーバ1（121）、2（122）を中継して、プロキシサーバ3（123）へ接続要求を送信し（ステップ506）、証明書1（141）を付けてプロキシサーバ3（123）へクライアントの認証要求を送信する（ステップ503）。

【0048】プロキシサーバ1（121）、2（122）は、それぞれステップ608でデータを中継する状態にあるから、クライアント（111）からのプロキシサーバ3（123）への接続要求、および認証要求は、プロキシサーバ1（121）、2（122）を経て、プロキシサーバ3（123）へ送られる。

【0049】プロキシサーバ3（123）は、図6の処理で接続待ち状態になっているので、クライアント（111）からの証明書1（141）付きの認証要求を受信し（ステップ601）、プロキシサーバ3（123）が属する認証サーバ3（133）へ接続し（ステップ602）、クライアント（111）の認証要求を証明書1（141）を付けて送信する（ステップ603）。

【0050】認証サーバ3（133）は、図7の処理で接続待ち状態になっているので、プロキシサーバ3（123）からのクライアント認証要求を受信し（ステップ701）、受信した証明書1（141）を用いて認証を行う（ステップ702）。認証サーバ3（133）では上述した処理により証明書1（141）が一時保存されているので認証は成功し、ステップ702から703に進む。また、認証要求元はクライアントであるので、図8の処理に進む（ステップ703）。図8において、証明書種別の判定（ステップ801）では、受け取った証明書1（141）は認証サーバ3（133）が管理する証明書ではないため、中継経路定義の検索は行わず、認証が成功した時点でプロキシサーバ2（122）へ認証

の成功を送信する（ステップ811）。認証終了後は、認証サーバ3（133）は証明書1（141）を破棄する。

【0051】プロキシサーバ3（123）は、認証サーバ3（133）から認証成功の通知を受信すると、ステップ604から605に進み、クライアント（111）に、認証の成功を通知する（ステップ605）。また、クライアント（111）から次の接続先であるサーバ（112）への接続要求を受信すると（ステップ607）、サーバ（112）へ接続して、データの中継を開始する（ステップ608）。

【0052】クライアント（111）は、プロキシサーバ3（123）からの認証成功の通知を受信すると、ステップ504から505に進み、次に中継するプロキシサーバは無いから、サーバへの接続要求を送信する（ステップ507）。このときプロキシサーバ1（121）、2（122）、3（123）は、何れもステップ608でデータを中継する状態にある。クライアント（111）は、サーバ（112）との通信を開始する（ステップ508）。通信が終了したら（ステップ509）、コネクションを切断する（ステップ510）。これにより、各プロキシサーバのコネクションも次々に切断される（ステップ609）。

【0053】クライアントの認証や、認証サーバ間の認証が失敗した場合は、失敗した時点で順次コネクションを切断し、クライアントアプリケーションにサーバへの接続失敗を通知する。

【0054】

【発明の効果】以上説明したように、本発明によれば、全ての中継するプロキシサーバが属する認証サーバから証明書を事前に配布しておく必要がなく、ユーザの管理が容易にできる。また、認証サーバを階層化して認証サーバグループを形成することにより、認証サーバグループの中で最初に認証要求を受信する下位の認証サーバ全てに設定しなければいけない中継経路を、上位の1台の認証サーバで管理することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態を示すシステム構成図。

【図2】各認証サーバに定義する、接続先サーバに対して次に中継するプロキシサーバの情報を持っている認証サーバを定義する説明図。

【図3】各認証サーバに定義する、接続先サーバへの接続を中継するプロキシサーバを定義する説明図。

【図4】各認証サーバに定義する、認証サーバのグループを構成するために上位の認証サーバを定義する説明図。

【図5】クライアントのVPNとしての動作を示すフローチャート図。

【図6】プロキシサーバの動作を示すフローチャート

【図7】認証サーバの動作を示すメインフローチャート図。

【図8】認証サーバがクライアントとの認証処理を示すサブフローチャート図。

【図9】認証サーバが認証サーバ間の認証処理を示すサブフローチャート図。

【符号の説明】

1 0 1, 1 0 2, 1 0 3, 1 0 4…それぞれ独立した(透過でない)ネットワーク1, 2, 3, 4。
1 1 1…クライアントアプリケーションが動作する計算機。
1 1 2…サーバアプリケーションが動作してクライアントからの接続を待機する計算機。

1 2 1, 1 2 2, 1 2 3…ネットワーク間を中継する計算機。

1 3 1, 1 3 2, 1 3 3, 1 3 4…クライアントのユーザ認証と認証サーバ間の認証を行う計算機。

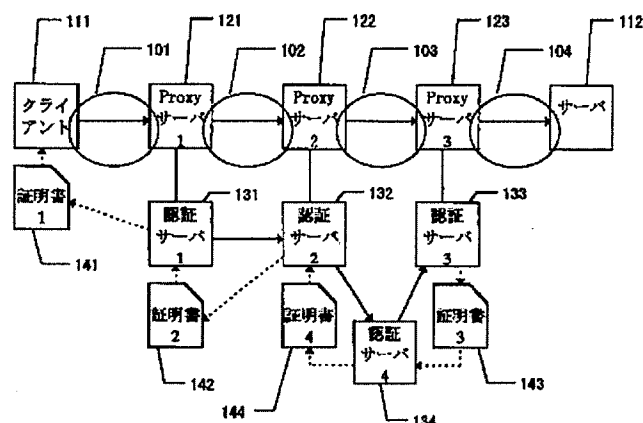
1 4 1…認証サーバ1からクライアントへ配布した証明書。

1 4 2…認証サーバ2から認証サーバ1へ配布した証明書。

1 4 3…認証サーバ3から認証サーバ4へ配布した証明書。

1 4 4…認証サーバ4から認証サーバ2へ配布した証明書。

【図1】



【図2】

認証サーバ	接続先	次の認証サーバ
認証サーバ1 (131)	サーバ(112)	認証サーバ2 (132)
認証サーバ2 (132)	—	—
認証サーバ3 (133)	サーバ(112)	End
認証サーバ4 (134)	サーバ(112)	認証サーバ3 (133)

(注) End : サーバと直接データの送受信が可能

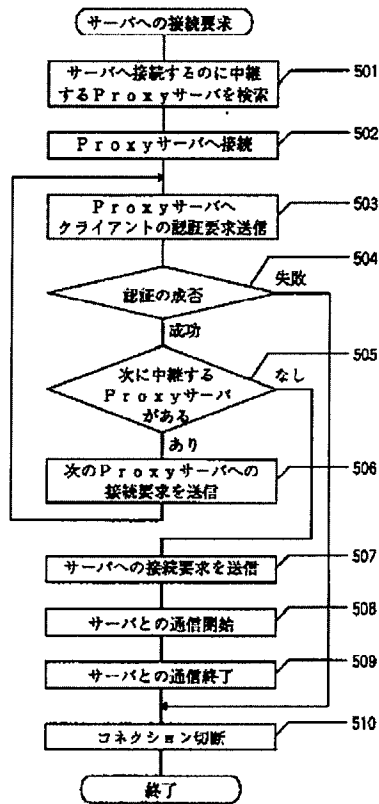
【図3】

認証サーバ	接続先	中継するProxyサーバ
認証サーバ1 (131)	サーバ(112)	Proxyサーバ1 (121)
認証サーバ2 (132)	サーバ(112)	Proxyサーバ2 (122)
認証サーバ3 (133)	サーバ(112)	Proxyサーバ3 (123)
認証サーバ4 (134)	—	—

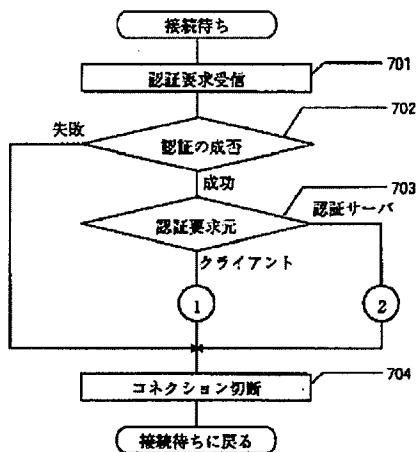
【図4】

認証サーバ	上位の認証サーバ
認証サーバ1 (131)	—
認証サーバ2 (132)	認証サーバ4 (134)
認証サーバ3 (133)	認証サーバ4 (134)
認証サーバ4 (134)	—

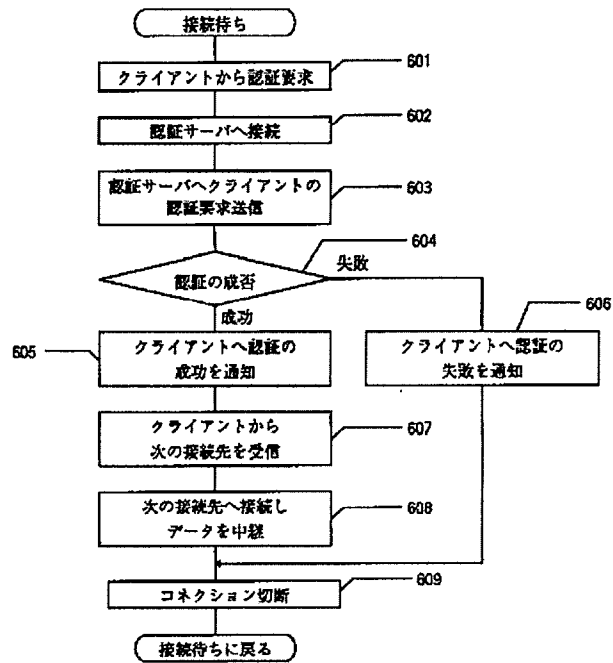
【図5】



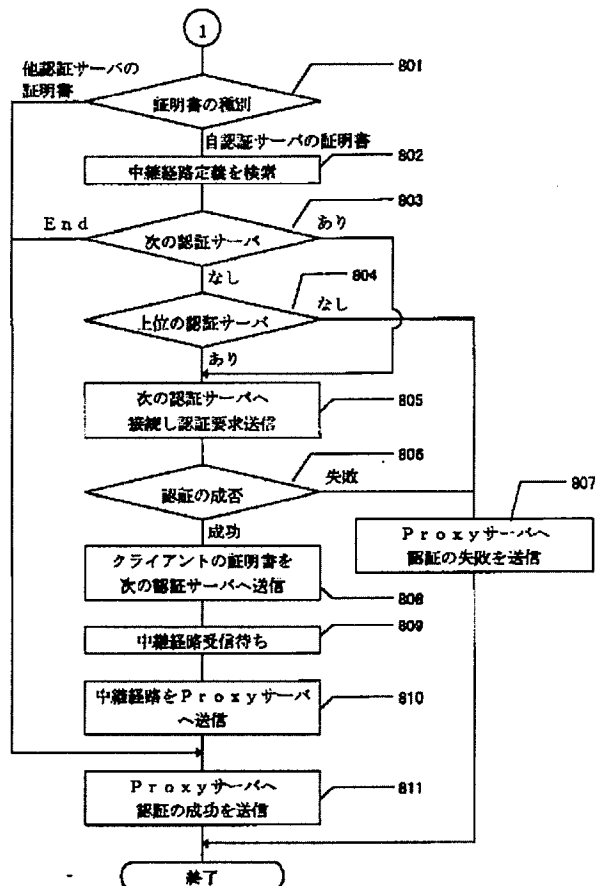
【図7】



【図6】



【図8】



【図9】

